Securing the Future:

The Critical Shift to High-Assurance Identity Verification

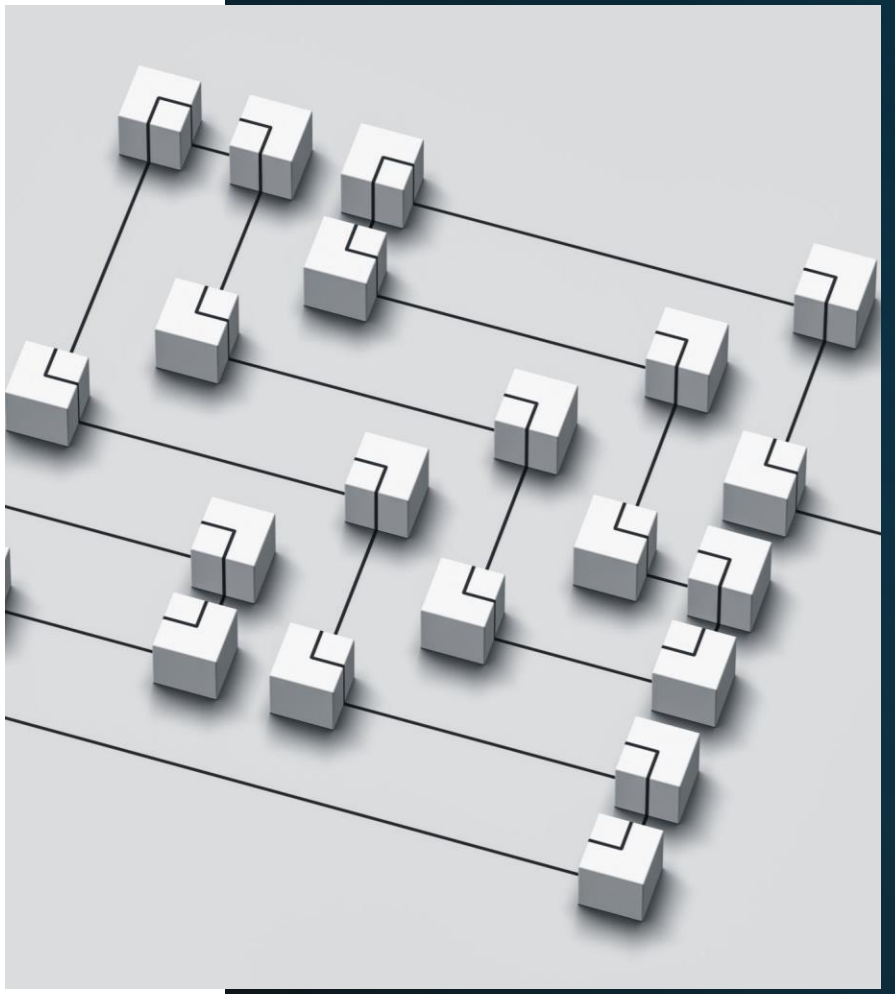
Juliana Cafik | Identity Standards & Solutions Architect

Identity Constructs

A **designed experience** through which an identity interacts with systems & services

Not **the identity itself**, but rather the **interface** that enables identity to be expressed

It can be physical or digital



Current Identity Construct: Framework for Interaction

Functional Layer: Interface between identity and systems

Separation Principle: Identity interaction with systems is distinct from the core identity

Contextual: Use case specific (e.g., opening a bank account, accessing health care, travel …)

What does the Current Identity Construct Do?

Identity Protection

Separating identity from its construct prevents compromise of the physical identity document

Governance

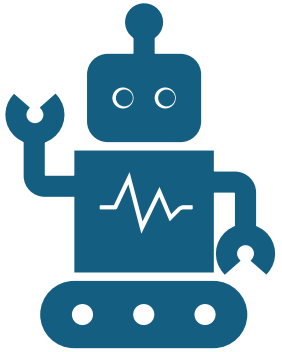
Constructs are governed independently, allowing for contextual policy enforcement and regulatory compliance (ie Payment, Travel, Open A Bank Account,…)

User Experience

Identity can be used across service providers while maintaining context. Creates common user experiences & promotes scaled adoption

Emergent Construct: Agentic AI

AI Agents observe, decide and act autonomously



AI Agents can be goal-oriented, adaptive and self improving

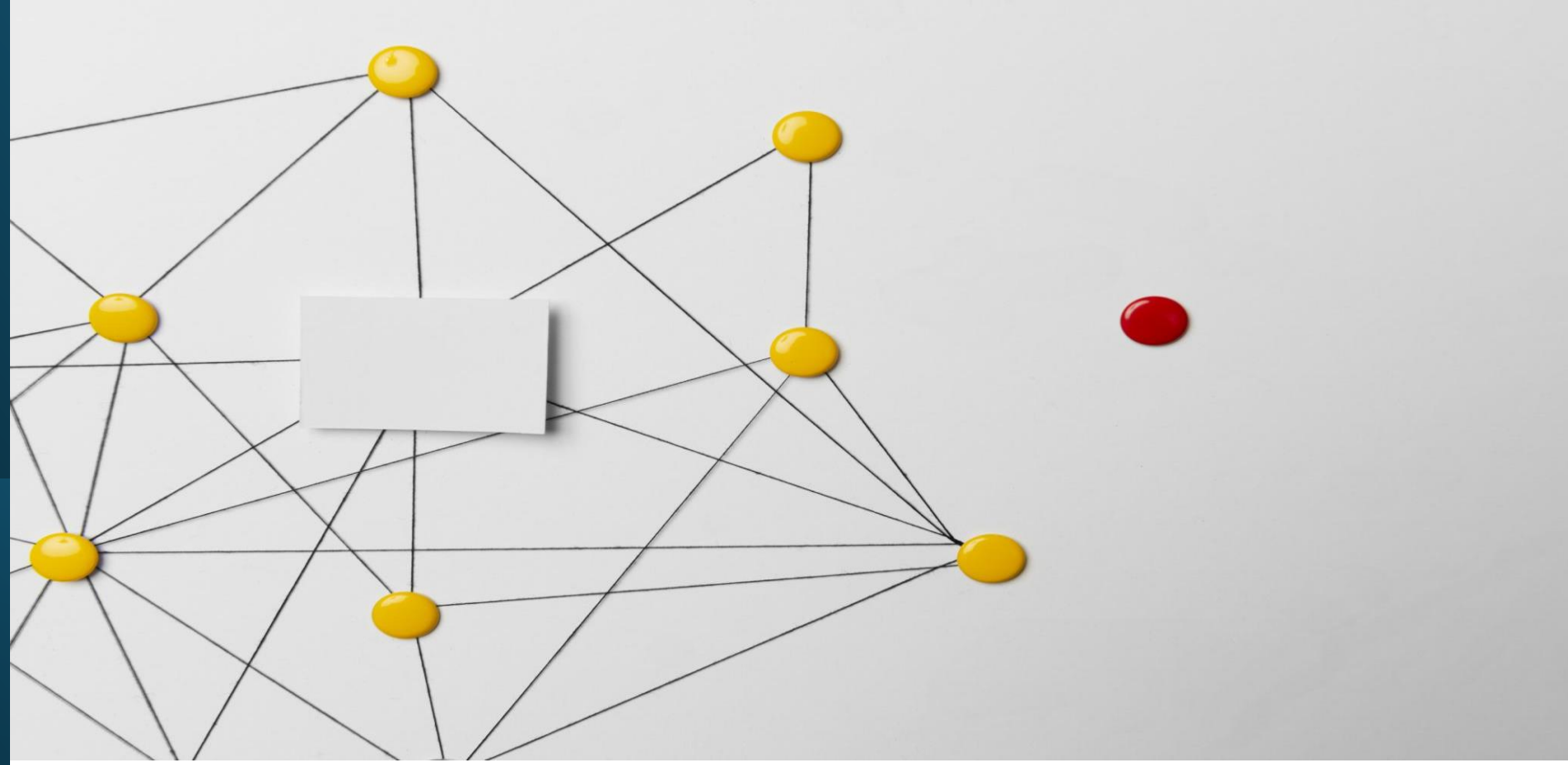
Agentic AI Exploitation of Current Identity Constructs
(examples)

Synthetic Identity Creation	GenAI to fabricate realistic identities by combining breached data with deepfake imagery
Deepfake-Driven Social Engineering	AI-generated voices and videos are used to impersonate individuals during onboarding or verification
AI Agents as Attack Surrogates	AI agents can autonomously exploit identity constructs by mimicking user behaviour or bypassing verification steps

Why are these Exploits so Effective?

The Construct is NOT Identity	Lack of Non-Repudiation	Fragmented Governance	AI Acceleration
Separation allows attackers to manipulate the construct without needing to ***verify identity***	Without ***cryptographic proof of origin,*** the existing identity construct can be spoofed	Lack of unified policy across platforms for ***verification & assurance***	***GenAI tools lower the barrier*** for creating convincing synthetic identities and attacks

Raising Identity Assurance



Enhancing assurance that a claimed identity can be cryptographically validated as the genuine identity of a distinct individual within a population

Epicenters of Effort

NIST NCCoE: Digital Identities - Mobile Driver’s License (mDL)

Building a New Identity Construct

High Assurance Identity Verification

Demonstrating the use of an mDL for establishing & accessing an online financial account to meet Customer Identification Program/Know Your Customer (CIP/KYC) Onboarding Requirements

NIST Publications

- **NIST SP 800-63A**: Digital Identity Guidelines – Enrollment and Identity Proofing
- **NIST SP 800-63A:** Profile for mDL Assurance
- **NIST SP 800-63B**: Authentication and Lifecycle Management
- **NIST SP 800-53 Rev. 5**: Security and Privacy Controls for Information Systems
- **NIST Privacy Risk Assessment Methodology (PRAM)**: Used to assess privacy risks in mDL implementations

OpenID Foundation Standards

- **OpenID Connect Core 1.0**: For identity assurance claims and authentication context
- **OpenID4VCI (Verifiable Credential Issuance)**: For credential exchange between issuers and wallets
- **SD-JWT (Selective Disclosure JWT)**: For privacy-preserving credential presentation

ISO/IEC Standards

- **ISO/IEC 18013-5**: International standard for mobile driving licences (mDL)
- **ISO/IEC 18013-7**: Defines server retrieval and remote presentation protocols
- **ISO/IEC 23220-4**: For mobile identity credentials

Regulatory and Compliance Frameworks

- **FFIEC BSA/AML Manual**: For financial institution compliance
- **CIP (Customer Identification Program)**: U.S. regulatory requirement for identity verification
- **GDPR**: European data protection regulation
- **eIDAS**: EU framework for electronic identification and trust services

Other Relevant Standards & Guidance

- **ETSI TS 119 461 V2.1.1 (2025-02)**: Electronic signatures and trust services
- **IANA AMR Registry (RFC 8176)**: Authentication method identifiers
- **AAMVA mDL Implementation Guidelines**: U.S. motor vehicle administration guidance
- **OAuTH 2.0**
- **FIDO**

STANDARDS

Stakeholder Collaboration

Issuer

Digital Wallet

Identity Service Provider

Financial Institution

Convey Assurance Across the Parties

NIST SP 800-63-4 + 800-63A Profile for mDL Issuance

New Work in OIDF: eKYC metadata

1.Requirements for eKYC metadata specification aligned with NIST SP 800-63A Profile for mDL to assist FI's in making access, or step-up, decisions during runtime

Considerations include:

- Referenceable by AAMVA, TSA and Financial Institutions
- REAL ID Compliance Indicator: NIST profile of ISO/IEC 18013-5 data elements aligned with AAMVA requirements including a DHS_compliance field in the mDL Mobile Security Object (MSO)
- NIST 800-63B Profile: Holder authentication metadata in the mDL presentation

2. Report on operational considerations ecosystem stakeholders can leverage via a shared metadata schema, designed to convey issuer-level identity assurance, in support of eKYC processes & CIP requirements

Contribute & Engage

- Provide feedback to NIST on draft guidance and publications
- Collaborate with standards bodies on ISO mDL (ISO, OIDF,…)
- Participate in technical workshops and interop testing